Authenticated Group Diffie-Hellman Key Exchange :

Theory and Practice

Olivier Chevassut (UCL - LBNL)

J.- J. Quisquater (UCL - Promotor)

D. Agarwal (LBNL - co-advisor, U.S.A)

D. Pointcheval (ENS - co-advisor, France)

Outline

✓ Introduction
  — motivation
  — research objectives

- Background
- Contributions
- Secure reliable multicast channels
- Provably secure group Diffie-Hellman key exchange
- Provably secure dynamic group DH key exchange
- Experimental results
- Conclusion and further work

Motivation

- An increasing number of distributed applications need to communicate within groups, e.g.
  - — collaboration and videoconferencing tools (Access Grid)
  - — distributed computations (Computational Grid)
  - — replicated servers
- An increasing number of distributed applications have security requirements
  - — privacy of data
  - — protection from hackers
  - — protection from viruses and trojan horses
- Group communication must address security needs

Research Objectives

- Provide an efficient and reliable communication between participants aggregated into a group
  - communication channel directly connecting the participants (no intermediary server)
  - remove dependence on centralized servers (bottleneck, scalability)
  - support participants spread across the Internet

- Provide a secure communication among the participants
  - support confidentiality, authenticity, and integrity
  - support access control based on certificates
  - security services optional

Outline

- Introduction
- ✓ Background
  - — secure reliable two-party communication channels
  - — algorithms for two-party Diffie-Hellman key exchange

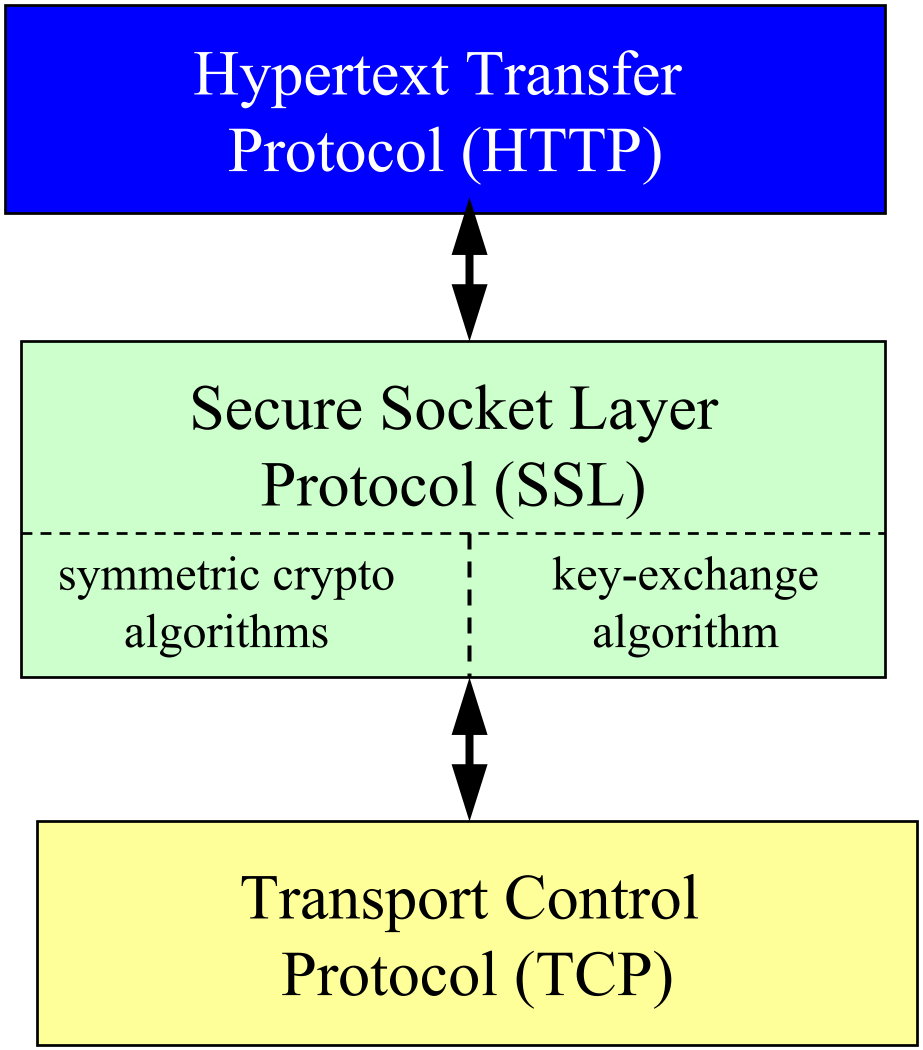
- Contributions
- Secure reliable multicast channels
- Provably secure group DH key exchange
- Provably secure dynamic group DH key exchange
- Experimental results
- Conclusion and further work

Secure and Reliable Two-Party Communication

- Provide an efficient and reliable communication between two participants
  - — communication channel connecting the participants
  - — client-server situation
  - — dependence on a centralized server (SSL, KDC)
  - — participants are spread across the Internet

- Provide a secure communication between the two participants supporting
  - — confidentiality, authenticity, and integrity
  - — authorization and access control
  - — security services optional

Secure Reliable Two-Party Communication : Architecture



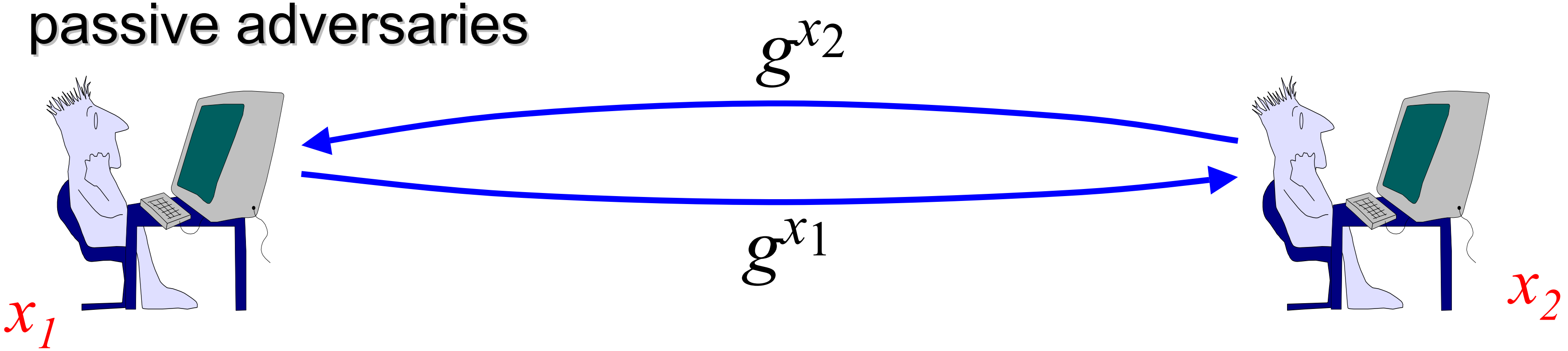
Secure Reliable Two-Party Communication : Components

- The Transport Control Protocol Layer (TCP)
  — provide SSL with reliable delivery of messages
  — provide SSL with fifo ordered delivery of messages
  — provide SSL with membership notifications

- The Secure Socket Layer Protocol (SSL)
  — symmetric crypto algorithms (e.g. Rijndael, and HMAC)
  — a key exchange algorithm enables the client and the server to establish a session key (e.g. DH, RSA)
  — access control based on certificates (Public-Key Infrastructure)

The Two-Party Diffie-Hellman Key Exchange

- Establishing a secure channel between a client and a server is reduced to the problem of generating a session key sk
- The session key is used to achieve data secrecy and integrity
- The original DH algorithm from 1976 was only secure against passive adversaries



$$\boxed{sk = g^{x_1 x_2}}$$

Designing Algorithms for Two-Party DH key Exchange

- Ad hoc or heuristic security
  - attack-response design not successful
  - helps avoid known attacks
- Formal Methods [BAN90]
  - formal specification tools
  - successful at finding flaws and redundancy
  - assurance limited to formal system
- Provable Security [GM85]
  - based on complexity theory
  - successful at avoiding flaws
  - useful to validate cryptographic algorithms

How Provable Security works

1. Specification of a model of computation

- instances of players are modeled via oracles
- adversary controls all interactions among the oracles
- adversary's capabilities are modeled by queries to the oracles
- adversary plays a game against the oracles

2. Definition of the security goals

- authentication, freshness and secrecy of session keys, forward-secrecy

3. Statement of the intractability assumptions

- computational/decisional Diffie-Hellman (CDH and DDH)

4. Description of the algorithm and its proof of security

- proof shows by contradiction that the algorithm achieves the security goals under the intractability assumptions

Contributions

1. [ACTT01] A framework for secure and reliable communication within peer-to-peer groups, IEEE Symposium on Computer and Communications, 2001

2. [BCPQ01a] Provable secure group DH key exchange, ACM Computer and Communications Security, 2001

3. [BCP01b] Provable secure dynamic group DH key exchange, Asiacrypt, 2001

4. [BCP02] Refinements - forward-secrecy, Eurocrypt, 2002

Outline

- Introduction
- Background
- Contributions

✓ Secure reliable multicast channels
  — a security framework to implement multicast channels
  — algorithms for group Diffie-Hellman key exchange

- Provably secure group Diffie-Hellman key exchange
- Provably secure dynamic group DH key exchange
- Experimental results
- Conclusion and further work

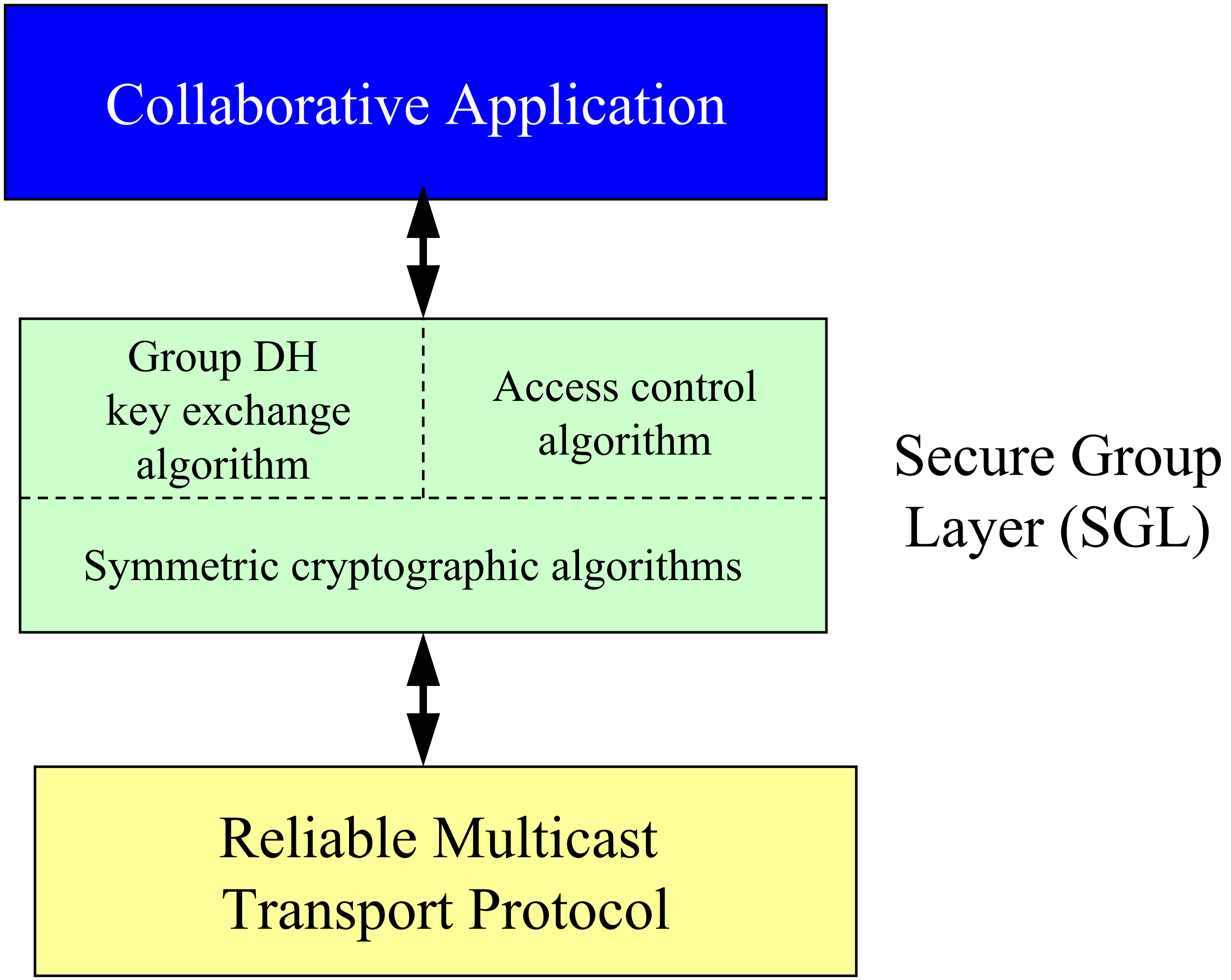
[ACTT01]
Security Framework (SGL)

- Symmetric crypto algorithms (e.g. Rijndael and HMAC)
  — implement an authenticated and encrypted channel

- An authenticated group DH key exchange algorithm enables group members to establish a session key

- A certificate-based access control mechanism makes sure that only the legitimate parties have access to the session key
  — off-line (does not participate in key exchange)

Secure Reliable Multicast Communication : Architecture



The Reliable Multicast Transport Layer

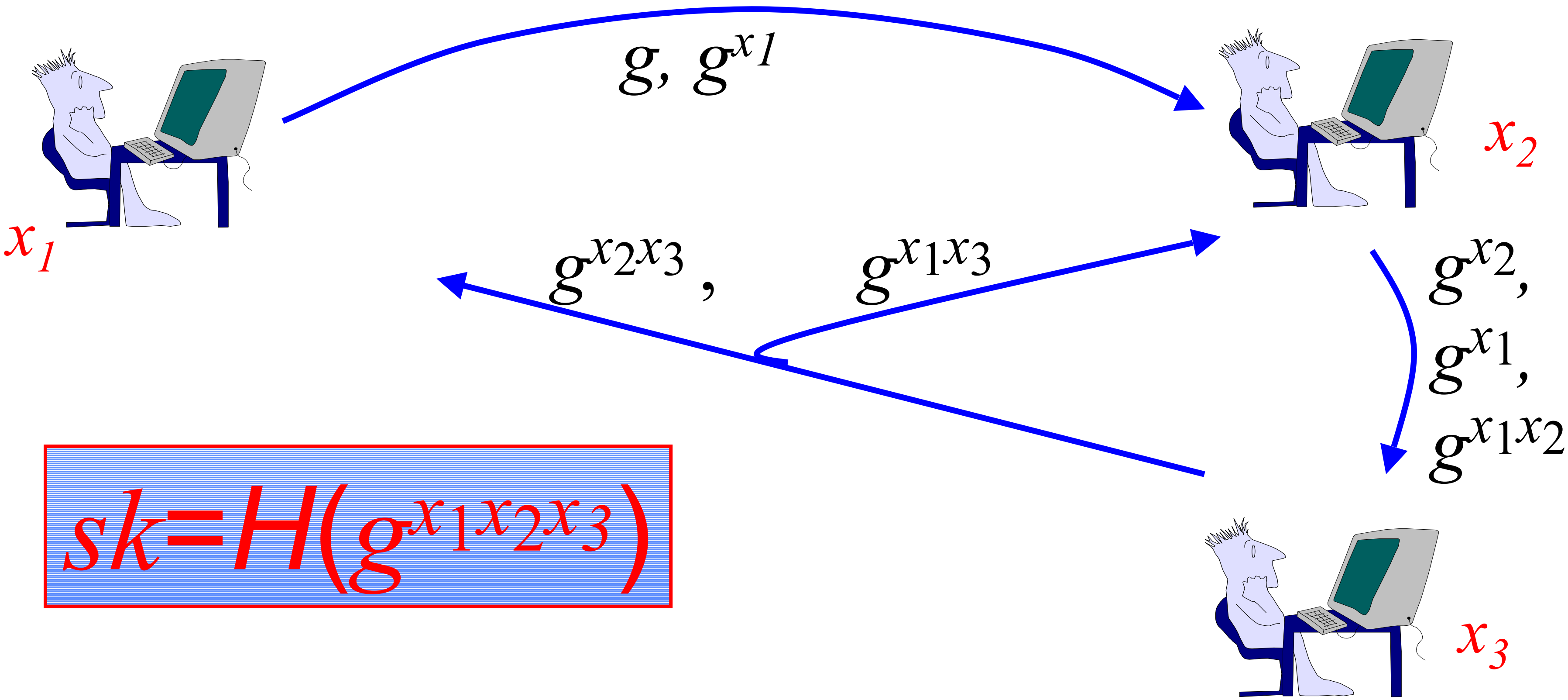
- Provide SGL with reliable and ordered delivery of messages
  - data messages are delivered in order - FIFO, partial, and total - at each member of the group
- Provide SGL with membership notifications
  - membership changes delivered in order with respect to data messages
- Several systems provide a reliable multicast layer
  - e.g., Isis, Ensemble, Totem and InterGroup

The Group Diffie-Hellman Key Exchange

- The session key is
  - $sk=H(g^{x_1 x_2 \ldots x_n})$
- Ring-based algorithm with signed flows :
  - up-flow: the contributions of each instance are gathered
  - down-flow: the last instances broadcasts the result
  - instances compute the session key from the broadcast

The Algorithm

- Up-flow: U_i raises received values to the power of x_i and forwards to U_{i+1}
- Down-flow: U_n processes the last up-flow and broadcasts



$$sk=H(g^{x_1 x_2 x_3})$$

Outline

- Motivation
- Background
- Contributions
- Secure reliable multicast channels

✓ Provably secure group Diffie-Hellman key exchange
  - — model of computation
  - — security goal of authenticated key exchange
  - — description of an algorithm and its proof of security

- Provably secure dynamic group DH key exchange
- Experimental results
- Conclusion and further work

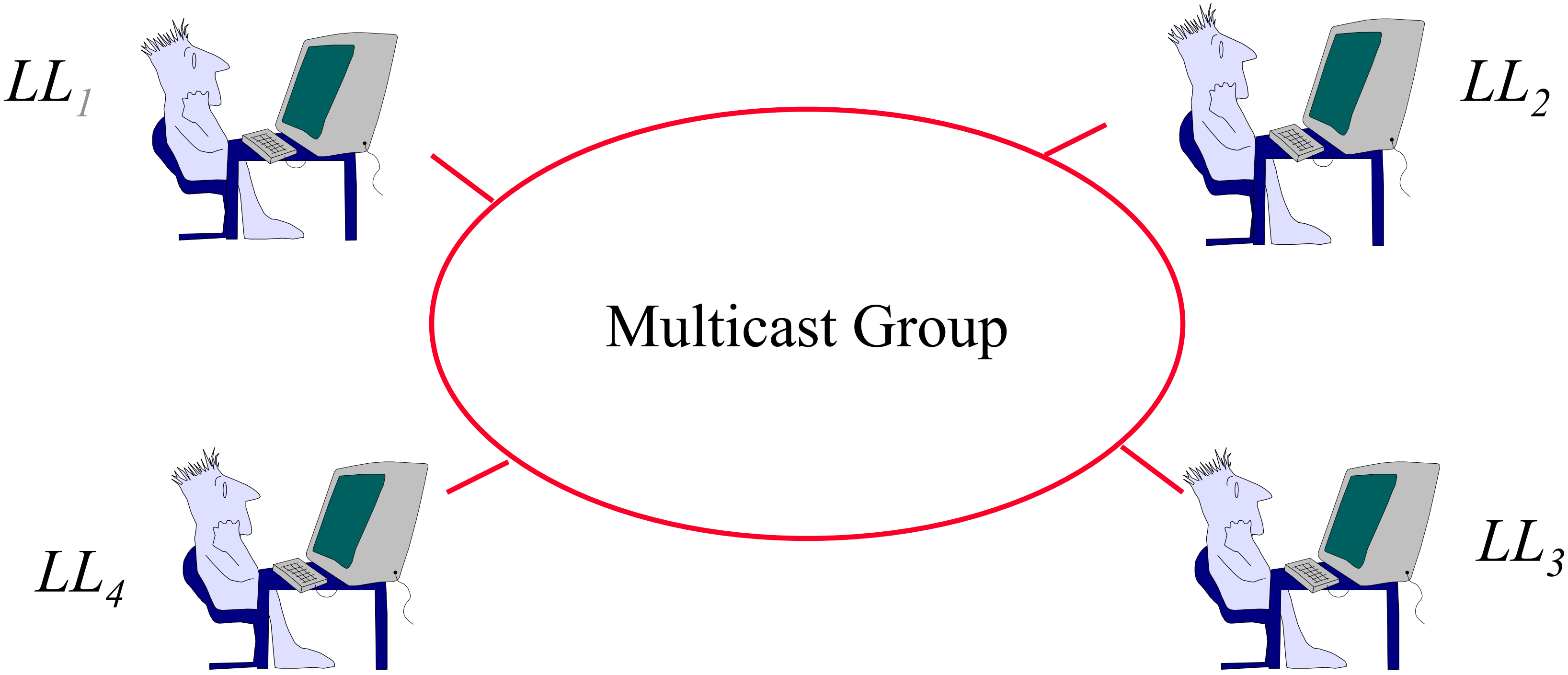
[BCPQ01a] Group Diffie-Hellman Key Exchange: The Setting

- Member characteristics
  - — small number of users (up to 100 members)
  - — members have similar computing power
  - — no hierarchy among members (no client/server)
  - — many-to-many communication

- Membership characteristics
  - — all members join the group at once
  - — membership participants are known in advance

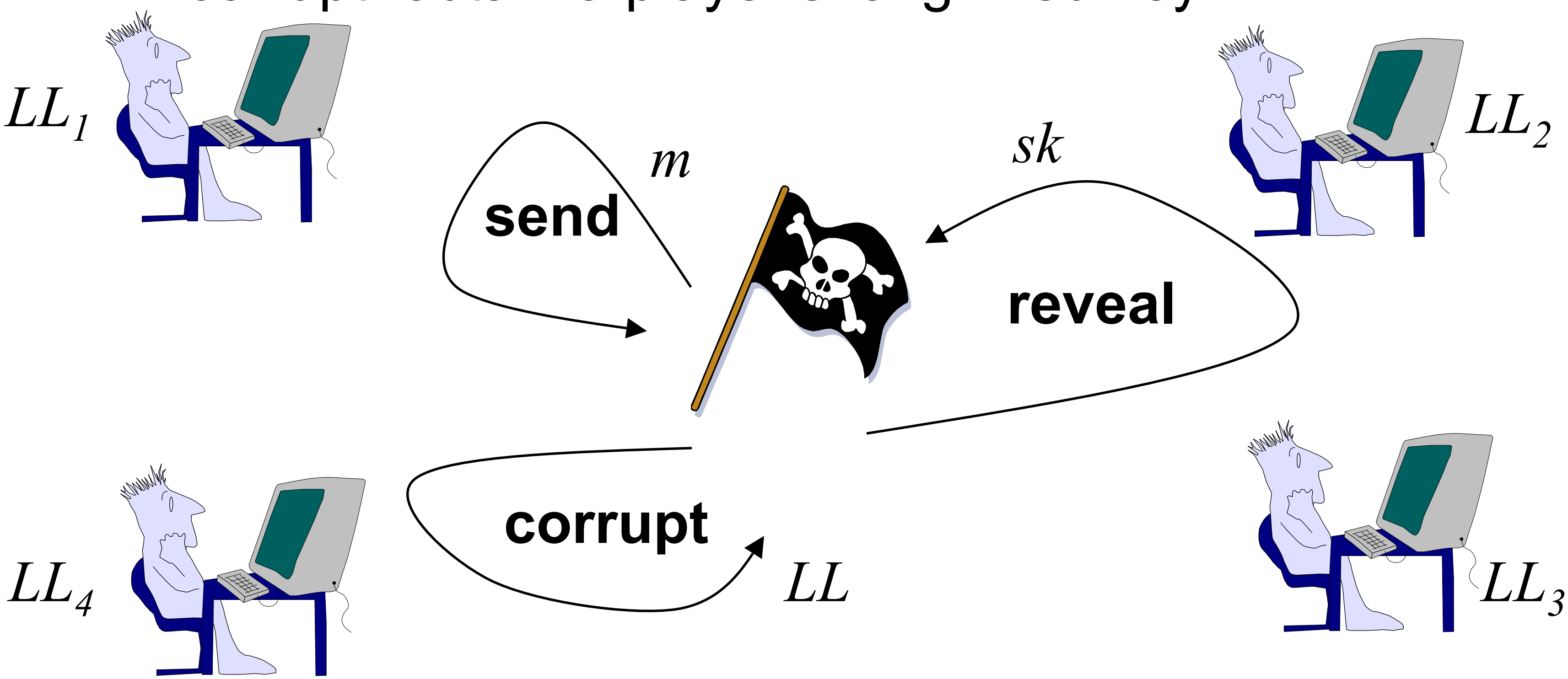
Model of Communication

- A multicast group consisting of a set of n players
  - each player is represented by many instances/oracles
  - each player holds a long-lived key (LL)

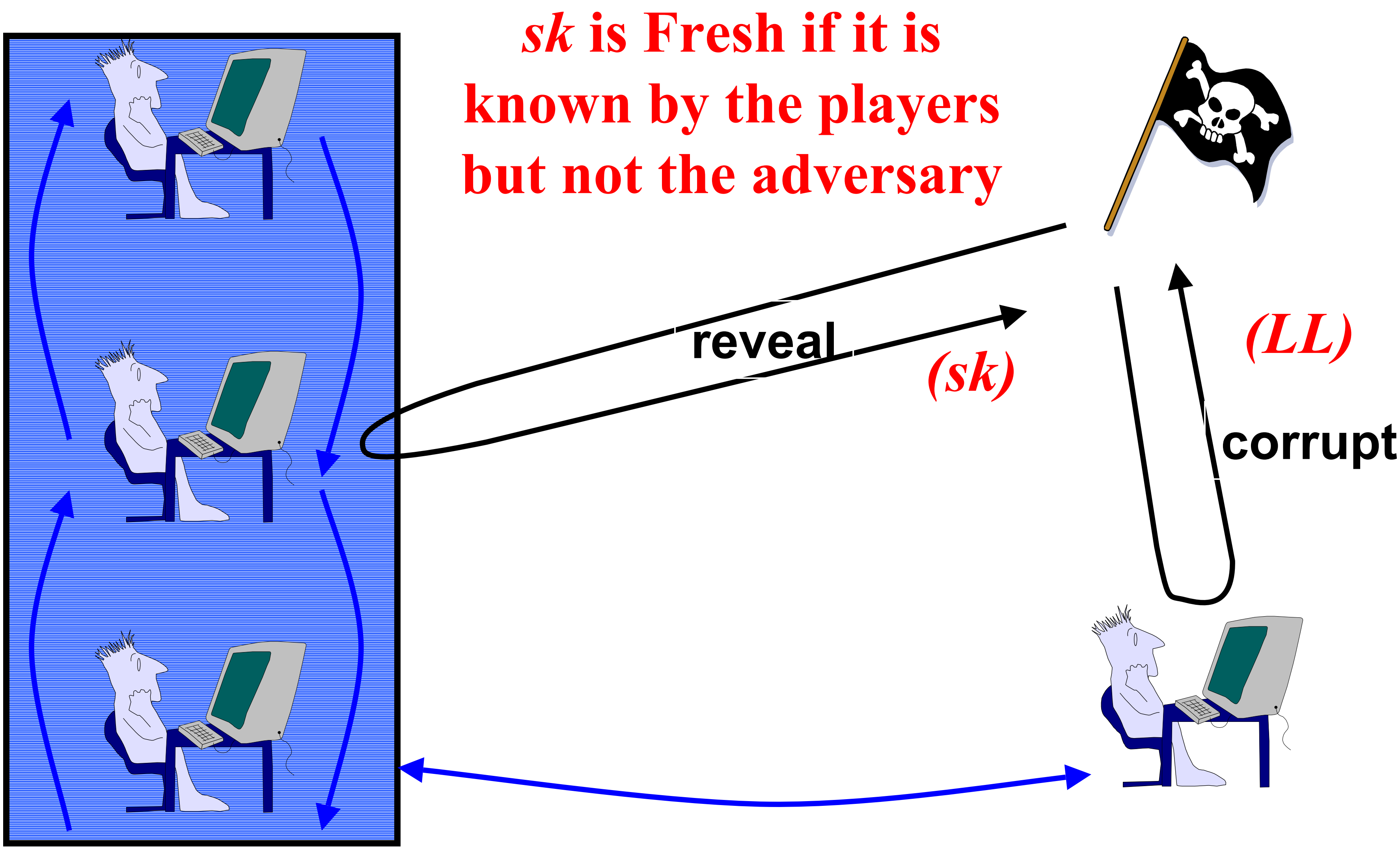


Modeling the Adversary

- Adversary's capabilities modeled through queries
  - — send: send messages to instances
  - — reveal: obtain an instance's session key
  - — corrupt: obtain a player's long-lived key



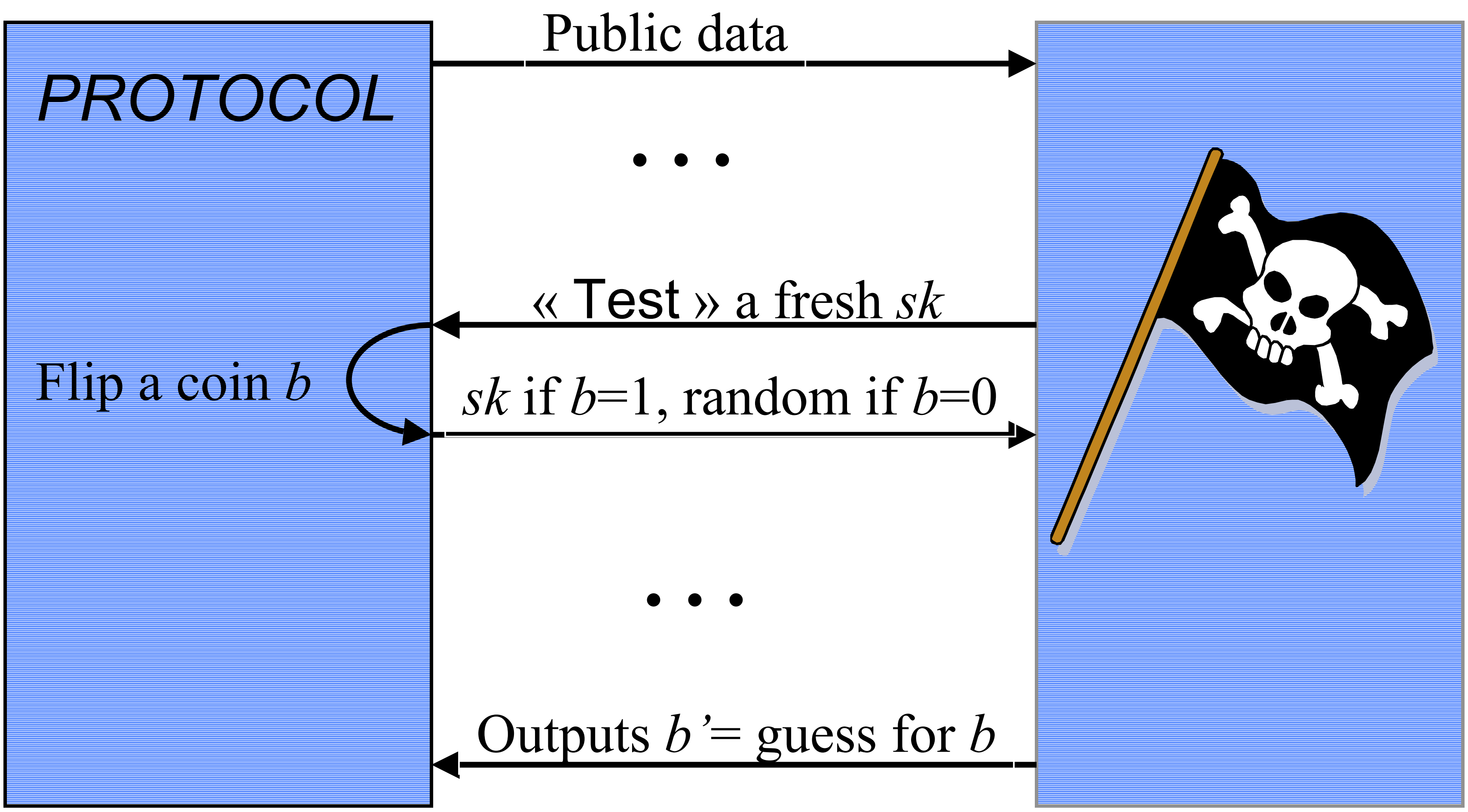
Freshness Related Queries



Security Goal : AKE
Authenticated Key Exchange

- Implicit authentication
  - Only the intended partners can compute the session key
- Semantic security
  - the session key is indistinguishable from a random string
  - modeled via a Test-query

Security Goal: The Game

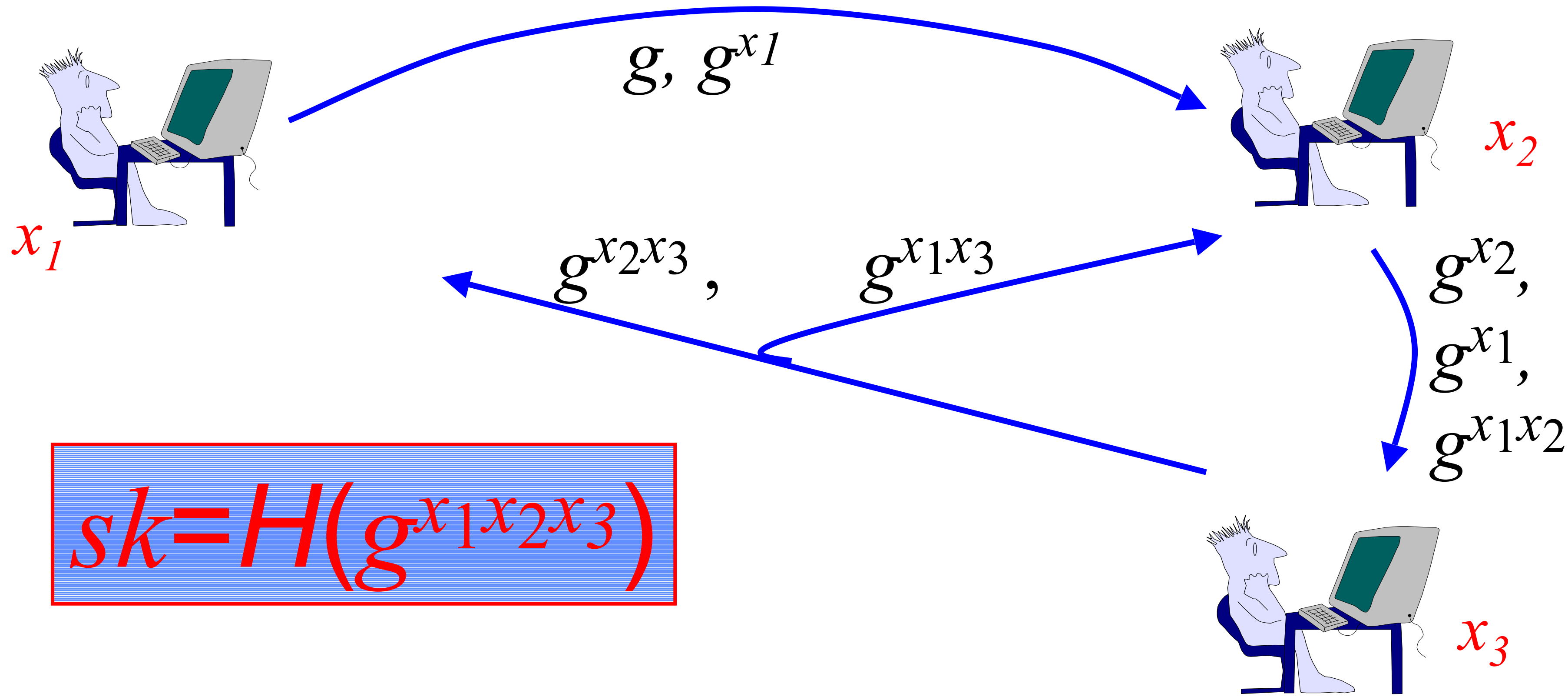


An Algorithm for Authenticated Group DH Key Exchange

- The session key is
  - $sk=H(g^{x_1 x_2 \ldots x_n})$
- Ring-based algorithm with signed flows :
  - up-flow: the contributions of each instance are gathered
  - down-flow: the last instances broadcasts the result
  - instances compute the session key from the broadcast
- Many details abstracted out

The Algorithm

- Up-flow: U_i raises received values to the power of x_i and forwards to U_{i+1}
- Down-flow: U_n processes the last up-flow and broadcasts



$$sk=H(g^{x_1x_2x_3})$$

Security Measurement

- Using ideal-hash assumption
- Theorem

  $\text{Adv}^{ake}(t, q_s, q_h) \leq n \cdot \text{Succ}^{cma}(t')$
  $+ \; 2 \cdot q_s^{\,n} \cdot q_h \cdot \text{Succ}^{gcdh}(t'')$

  $t', t'' \leq t + q_s \cdot n \cdot T_{exp}(k)$

- The adversary can break the algorithm in two ways

  (1) the adversary forges a signature w.r.t some player's LL-key => it is possible to build a forger (CMA)

  (2) the adversary is able to guess the bit b involved in the Test-query => it is possible to solve an instance of the GCDH problem

Outline

- Motivation
- Background
- Contributions
- Secure reliable multicast channels
- Provably secure Group DH key exchange

✓ Provably secure dynamic group DH key exchange
  - — model of computation
  - — description of an algorithm and its proof of security

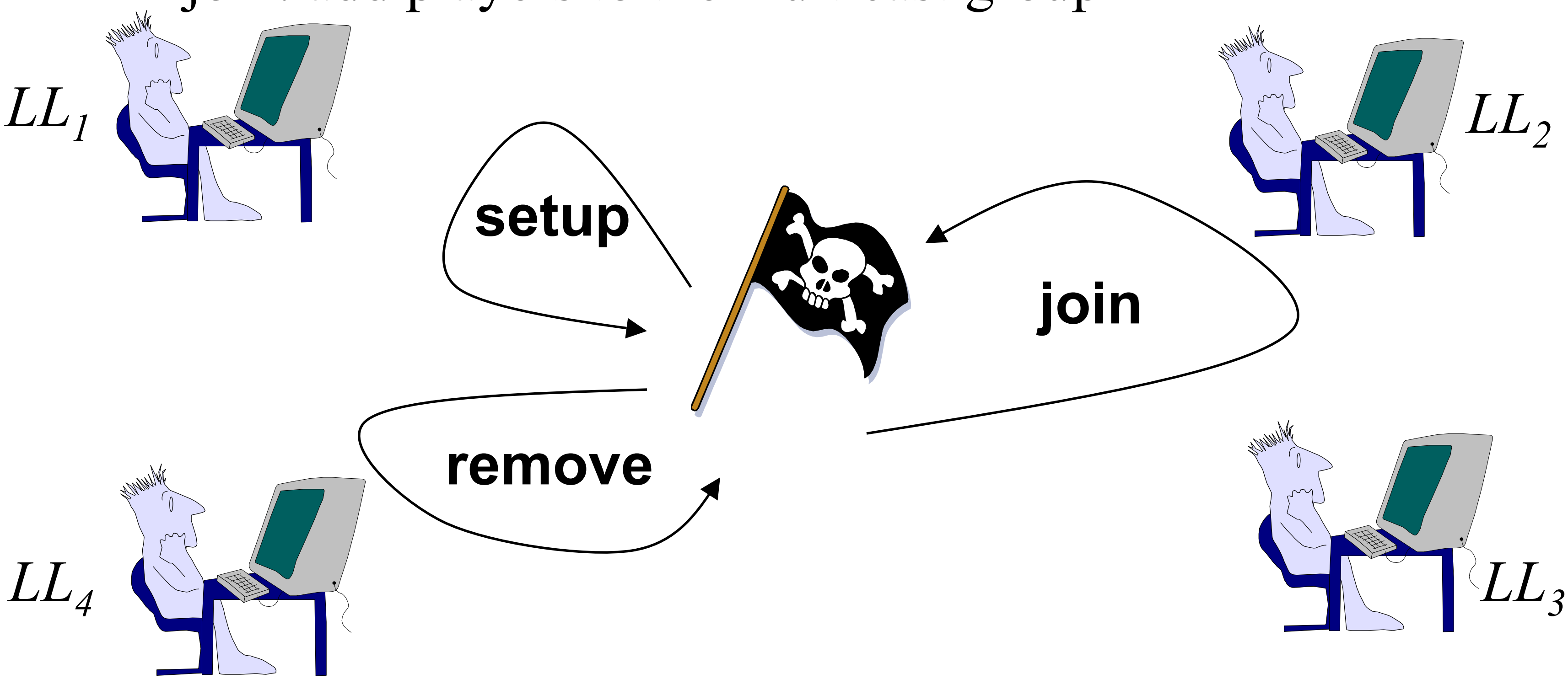
- Experimental results
- Conclusion and further work

[BCP01b] Dynamic Group DH key Exchange: The Setting

- Additional membership characteristics
  - — members join and leave the group at any time
  - — network partitions and merges (i.e asynchronous network with failures)
  - — membership is incrementally defined

Modeling the Adversary

- Adversary's additional queries
  - setup: initialize the multicast group
  - remove: remove players from multicast group
  - join: add players to the multicast group

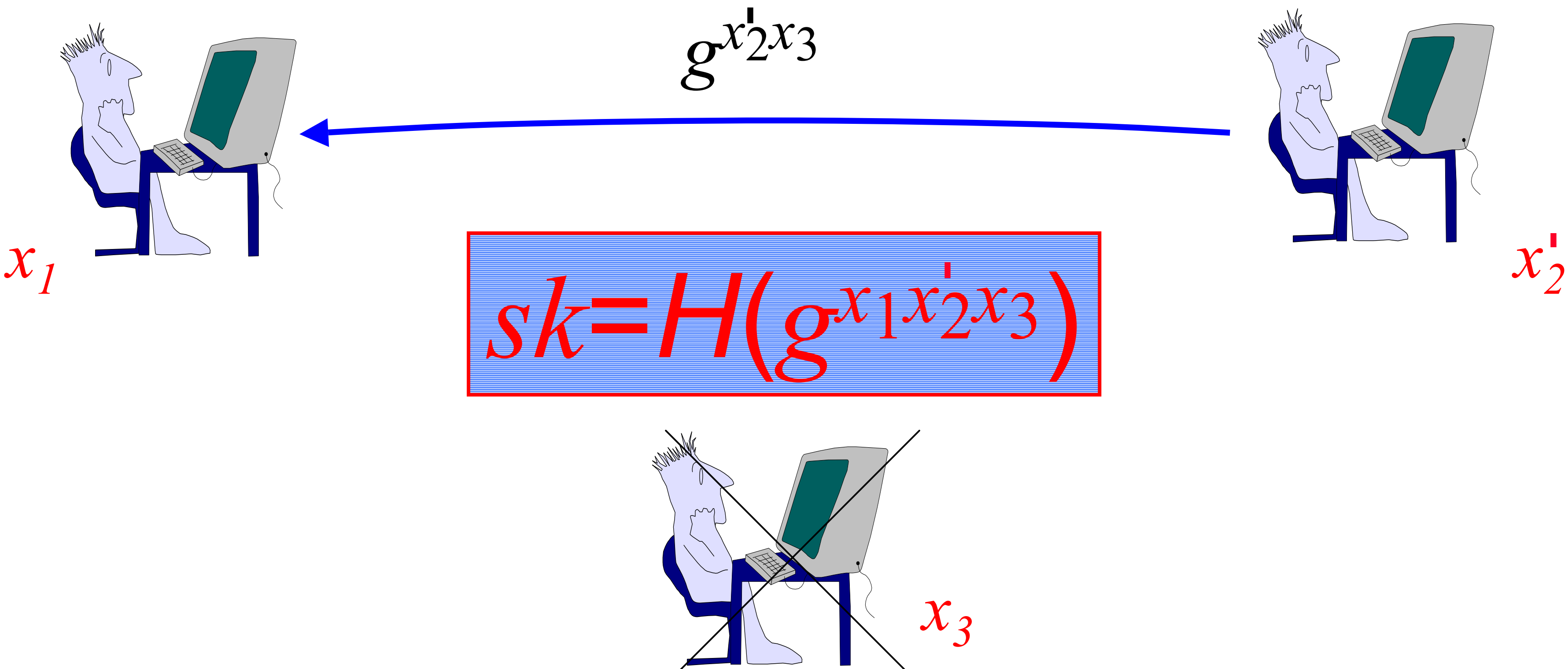


An Algorithm for Authenticated Dynamic Group DH Key Exchange

- The session key is
  - $sk = H(g^{x_1 x_2 \dots x_n})$
- Ring-based with signed flows
- Defined by two additional algorithms
  - JOIN
  - REMOVE
- Many details abstracted out

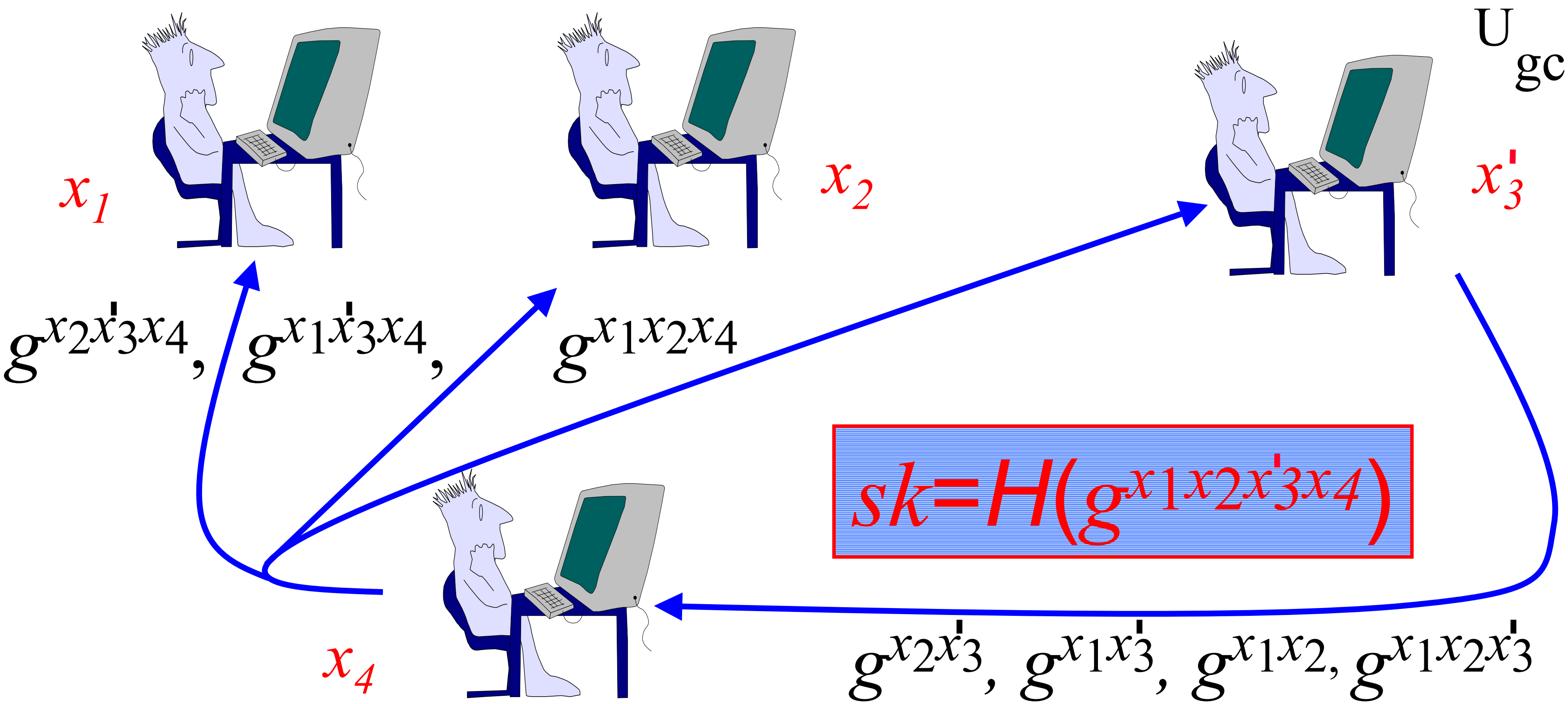
The REMOVE Algorithm

- Down-flow: player with highest index (U_{gc}) raises the previous saved broadcast to the power of its new private exponent and broadcast the result



The JOIN Algorithm

- Up-flow : U_{gc} raises the previous saved broadcast to the power of its new private exponent and forwards to U_{i+1}
- Down-flow: U_n processes the last up-flow and broadcasts



Security Measurement: Authenticated Key Exchange (AKE)

- Ideal-hash assumption
- Theorem

$$\mathrm{Adv}^{ake}(t, Q, q_s, q_h) \leq 2 \cdot n \cdot \mathrm{Succ}^{cma}(t') + 2 \cdot Q \cdot \binom{n}{s} \cdot s \cdot q_h \cdot \mathrm{Succ}^{gcdh}(t'')$$

$$t', t'' \leq t + (Q + q_s) \cdot n \cdot T_{exp}(k)$$

- The adversary can break the protocol in two ways

  (1) the adversary forges a signature w.r.t some player 's LL-key => it is possible to build a forger (CMA)

  (2) the adversary is able to guess the bit b involved in the Test-query

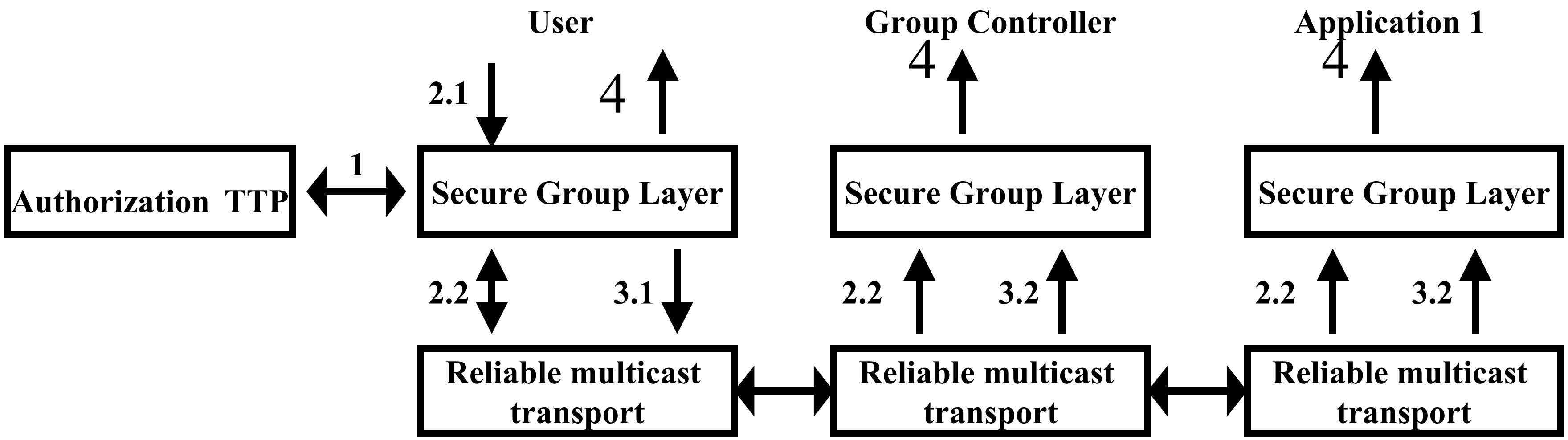
  => it is possible to come up with an algo that solves an instance of the GCDH problem

Outline

- Motivation
- Background
- Contributions
- Secure reliable multicast channels
- Provably secure group DH key exchange
- Provably secure dynamic group DH key exchange
- ✓ Experimental results

- Conclusion and further work

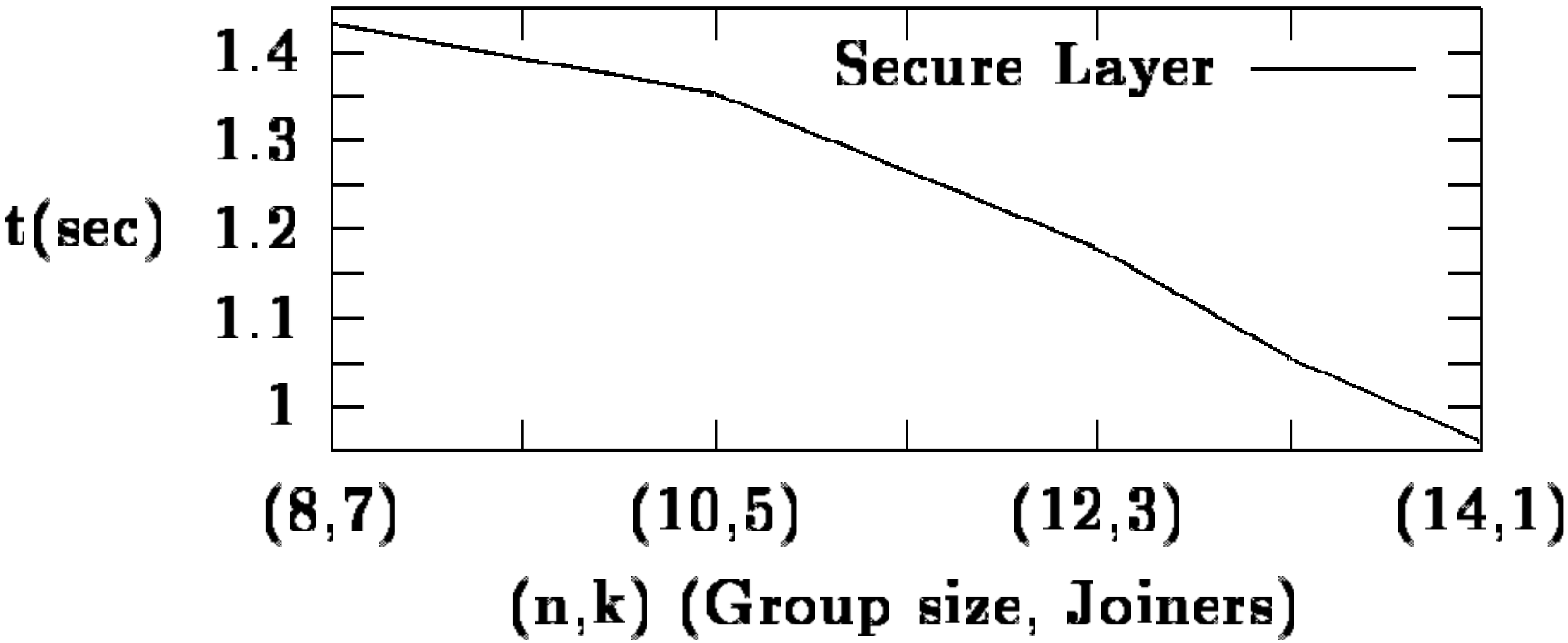
The Access Control Algorithm in SGL : a user join



1. **Authorization:** The user requests its permission from TTP and obtains a membership authorization certificate
2. **Join multicast group**:
   2.1.The user submits a join request
   2.2. Secure Group Layer gets a membership change notification
3. **Access control**:
   3.1. The user broadcasts its certificate
   3.2. U_{gc} checks the user's permission and, if authorized, initiates group DH key exchange
4. **Deliver secure membership**: When the group DH key exchange is done, Secure Group Layer delivers the secure membership notification to the application

A Preliminary Implementation of SGL

- Implementation in C : Totem, GDH with DSA, Akenti
- Performance : group size = 15 members, merge operation with variable-size sub-groups.



Conclusion

- Completed
  - [ACTT01] “An Integrated Solution for Secure Group Communication in Wide-Area Networks”, IEEE Symposium on Computers and Communication’01
  - [BCPQ01a] “Authenticated GDH key exchange: the static case”, ACM CCS’01
  - [BCP01b] “Authenticated GDH key exchange: the dynamic case”, Asiacrypt’01
  - [BCP02a] “Forward secrecy in GDH key exchange”, Eurocrypt’02
- Other related publications
  - [BCPPQ02] “Two Views of Authenticated GDH Key Exchange”, DIMACS Cryptographic Protocols in Complex Environments, 2002

Conclusion

- [BCP02b] "The Group Diffie-Hellman Problems", SAC'02
- [BCP02c] "GDH Key Exchange secure against dictionary attacks", Asiacrypt'02
- [BAC02] "A Practical Approach to the InterGroup Protocols", J. of Future Generation Computer Systems, 2002

- Current and on-going work
  - SGL security improvements, and delivery semantics
  - Demonstration of an application using SGL and InterGroup Protocols